สุขภาพที่ดีของมนุษย์

เทคโนโลยีสารสนเทศ

เคารพความแตกต่างของกันและกัน

อิสระในการทำงานและการใช้ชีวิตส่วนบุคคล

เชื่อมั่นในตัวท่านในฐานะที่เป็นผู้ใหญ่

พูดความจริงในสิ่งที่เราทำทุกวัน

คำมั่นสัญญาของเมก้า คือ

การจัดหาผลิตภัณฑ์
และให้บริการที่มีคุณภาพแก่ลูกค้า

โดยผ่านการพัฒนาและปรับปรุงนวัตกรรม
อย่างต่อเนื่อง

1 บทนำ

เรารู้สึกเป็นเกียรติที่ได้ทำงานในหนึ่งในองค์กรที่ดีสุด ถือเป็นหน้าที่และความรับผิดชอบสูงสุดของเราในการรักษาและเสริมสร้างชื่อเสียงขององค์กรไปทั่วโลก ในตลอดช่วงหลายปีที่ผ่านมาเราประสบความสำเร็จบนรากฐานที่แข็งแกร่งซึ่งเกิดจากความยั่งยืน การดำเนินการที่โปร่งใสและความถูกต้องตามหลักจริยธรรมในการดำเนินธุรกิจและการมีสินค้าที่มีคุณภาพภารกิจในการสร้างการเติบโตขององค์กรนั้นเป็นไปในทิศทางเดียวกันกับพันธสัญญาของเราที่จะซื่อสัตย์ในทุกๆความสัมพันธ์ ไม่ว่าจะเป็นความสัมพันธ์ระหว่างพนักงาน ลูกค้า ผู้ผลิต รัฐบาล ชุมชน รวมถึงผู้ที่เกี่ยวข้อง และผู้ถือหุ้น

วัตถุประสงค์ของข้อมูลเทคโนโลยีสารสนเทศ คือ การดำเนินธุรกิจอย่างมีประสิทธิภาพผ่านการบริหารดูแลกิจการที่ดี และสร้างสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศที่ปลอดภัยและมั่นคงในบริษัทฯ โดยหลักจรรยาบรรณนี้นำมาใช้กับกรรมการผู้บริหาร ฝ่ายจัดการและพนักงานทุกคนของบริษัท เมก้า ไลฟ์ไซแอนซ์ จำกัด (มหาชน) และบริษัทย่อย บริษัทร่วม และผู้ที่ได้รับมอบหมายของบริษัท(“เมก้า”)ทั้งนี้ เมก้าให้การสนับสนุนอย่างเต็มที่ในการนำหลักจรรยาบรรณนี้ไปใช้เพื่อประโยชน์ของบริษัท

2 การกำกับดูแลกิจการ

นโยบายนี้ มีวัตถุประสงค์เพื่อให้แน่ใจว่าเมก้าได้กำกับดูแลกิจการโดยการดึงจุดแข็งและข้อดีของเทคโนโลยีสารสนเทศมาใช้ได้อย่างมีประสิทธิภาพและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้สอดคล้องกับความเสี่ยงโดยรวมขององค์กรโดยทรัพยากรเทคโนโลยีสารสนเทศสามารถเชื่อมโยงและควบคุมได้ เพื่อให้แน่ใจว่าเมก้าสามารถบรรลุเป้าหมายรวมถึงกลยุทธ์และการดำเนินการพร้อมนโยบายและการตัดสินใจในการใช้กลยุทธ์ดังกล่าวเทคโนโลยีสารสนเทศจำเป็นต้องมีการจัดการความเสี่ยงการรายงานและการตรวจสอบที่เหมาะสมเพื่อให้แน่ใจว่าเทคโนโลยีที่นำมาใช้ สามารถส่งเสริมกลยุทธ์และนำองค์กรไปสู่ความสำเร็จตลอดจนการแข่งขันและการเพิ่มมูลค่าทางธุรกิจ นโยบายด้านเทคโนโลยีสารสนเทศกำหนดขอบเขตของเรื่องที่จะช่วยให้บรรลุวัตถุประสงค์ดังกล่าวเมก้าได้จัดทำนโยบายนี้ขึ้นมาเป็นลายลักษณ์อักษร และมีการสื่อสารนโยบายนี้ให้แก่ทุกคนที่ใช้เพื่อให้บรรลุเป้าหมายตามวัตถุประสงค์ที่ระบุไว้ในที่นี้นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 1 ธันวาคม พ.ศ. 2564 และ เมก้าหรือคณะกรรมการบริษัท/ คณะผู้บริหารของบริษัทมีสิทธิที่จะแก้ไขนโยบายนี้ได้เป็นครั้งคราว

3 การบริหารจัดการความเสี่ยง

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจะสอดคล้องกับนโยบายการบริหารความเสี่ยงขององค์กรและต้องครอบคลุมประเด็นต่อไปนี้

1. กำหนดบทบาทและหน้าที่ความรับผิดชอบในการบริหารความเสี่ยงในด้านเทคโนโลยีสารสนเทศ

ผู้จัดการ– หัวหน้าทีมเทคโนโลยีสารสนเทศจะเป็นเจ้าของความเสี่ยงและรับผิดชอบในการจัดการความเสี่ยงรวมถึงการบรรเทาความเสี่ยง

2. ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

- ความเสี่ยงทางกายภาพและสภาพแวดล้อมของห้องข้อมูลที่มีเซิร์ฟเวอร์ การเชื่อมต่อเครือข่ายและอุปกรณ์อื่นๆติดตั้งอยู่การเข้าถึงห้องนี้ได้จะต้องอยู่ภายใต้การควบคุม รวมถึงระบบควบคุมอุณหภูมิและระบบเตือนภัยอัคคีภัย

- ความเสี่ยงที่เกี่ยวข้องกับการใช้ซอฟต์แวร์ในคอมพิวเตอร์ของบริษัทเพื่อป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ปลอดภัยหรือเป็นอันตราย ตัวอย่างเช่น อาจทำให้มีโปรแกรมไม่พึงประสงค์ที่เป็นอันตราย (มัลแวร์) หรือไวรัสคอมพิวเตอร์ หรือปล่อยให้มีการโจมตีจากเครือข่ายภายนอกในเครื่องหรือเครื่องอื่นๆที่ทำงานในเครือข่ายเดียวกัน

- ความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเครือข่ายของบริษัท: เครือข่ายภายในและระบบอินเทอร์เน็ตจะต้องได้รับการตรวจสอบและเฝ้าระวังด้วยกระบวนการปิดกั้นการเข้าถึงเซิฟเวอร์และเครื่องลูกข่ายโดยบุคคลภายนอกซึ่งต้องมีการตรวจสอบการใช้งานอินเทอร์เน็ต การติดตั้งซอฟต์แวร์ป้องกันไวรัส การคัดกรองอีเมลที่รับมาและส่งออกไป ฯลฯ

- ความเสี่ยงส่วนบุคคลที่จำเป็นต้องมีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ อุปกรณ์และข้อมูลตามบทบาทของตน เพื่อป้องกันการแก้ไขหรือการเปลี่ยนแปลงข้อมูล

3. การประเมินความเสี่ยงจะครอบคลุมถึงความน่าจะเป็นและผลกระทบที่เป็นไปได้ เพื่อจัดลำดับความสำคัญของการบริหารความเสี่ยง โดยความเสี่ยงได้แบ่งออกเป็น 4 ประเภท ดังนี้

- ความเสี่ยงทางเทคนิคที่อาจเกิดขึ้นจากการโจมตีคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

- ความเสี่ยงที่เกี่ยวข้องกับผู้ใช้งาน อาจเกิดขึ้นได้จากการระบุสิทธิ์ของผู้ใช้งานที่ไม่เหมาะสมโดยอนุญาตให้เข้าถึงเกินขอบเขตของความรับผิดชอบและอาจทำให้เกิดความเสียหายต่อข้อมูล

- ความเสี่ยงจากภัยพิบัติและเหตุฉุกเฉินที่เกิดขึ้นจากมนุษย์หรือภัยธรรมชาติ และสถานการณ์อื่นๆ เช่น ไฟฟ้าดับและการประท้วง

- ความเสี่ยงที่เกี่ยวข้องกับการจัดการที่เกิดจากความไม่สอดคล้องกันของแนวทางที่มีอยู่กับความเสี่ยงที่อาจเกิดขึ้นได้

4. วิธีการหรือเครื่องมือที่กำหนดวิธีการควบคุมความเสี่ยงภายในของบริษัท

จัดทำคำอธิบายเกี่ยวกับความเสี่ยงซึ่งประกอบไปด้วย หัวข้อ ชื่อความเสี่ยง ประเภทของความเสี่ยง คำอธิบาย ปัจจัยเสี่ยง ผลกระทบ ฯลฯ การแจกแจงความน่าจะเป็น และคาดการณ์ความรุนแรงของผลกระทบและจัดทำแผนภูมิความเสี่ยง

5. ระบุตัวชี้วัดความเสี่ยงด้านไอทีและระบบการตรวจสอบตัวชี้วัดเหล่านี้และรายงานผลไปยังผู้รับผิดชอบ เพื่อที่ความเสี่ยงสามารถถูกจัดการได้อย่างเหมาะสมและทันท่วงที

4 ความปลอดภัย

1. แนวทางเพิ่มเติมเกี่ยวกับนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศและมาตรการรักษาความปลอดภัย

- วัตถุประสงค์

เพื่อป้องกันการละเมิดนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

- แนวทางปฏิบัติ

- ห้ามใช้ทรัพยากรคอมพิวเตอร์และเครือข่ายเพื่อกระทำการใดๆที่ละเมิดต่อกฎหมายหรือผิดศีลธรรมเช่น การสร้างเว็บไซต์เพื่อจำหน่ายหรือส่งเสริมสิ่งที่ผิดกฎหมายและบรรทัดฐานทางศีลธรรม

- ไม่ใช้บัญชีผู้ใช้หรือเครือข่ายคอมพิวเตอร์ของผู้อื่น ไม่ว่าจะได้รับอนุญาตจากเจ้าของบัญชีหรือไม่ก็ตาม

- ห้ามเข้าถึงระบบคอมพิวเตอร์หรือเข้ารหัสข้อมูลของบุคคลอื่นเพื่อแก้ไข ลบ เพิ่ม หรือคัดลอกข้อมูล

- ห้ามเปิดเผยข้อมูลของบุคคลอื่นหรือข้อมูลขององค์กรโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

- ห้ามขัดขวาง ทำให้เสียหาย หรือทำลายทรัพยากรคอมพิวเตอร์และเครือข่ายของบริษัท โดยการแพร่ไวรัสคอมพิวเตอร์หรือเข้าโปรแกรมที่ทำให้คอมพิวเตอร์เครือข่ายหรืออุปกรณ์ไม่สามารถใช้งานได้ (DOS) ฯลฯ

- ห้ามลักลอบขนส่งข้อมูลจากเครือข่ายของบริษัทหรือเครื่องอื่นๆที่เชื่อมต่อกับเครือข่ายเพื่อการรับส่งข้อมูล

- เปิดใช้งานซอฟต์แวร์ป้องกันไวรัสไว้อย่างเสมอก่อนเปิดไดรฟ์แบบพกพา ไฟล์แนบอีเมล และไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ต

- ผู้ใช้ต้องไม่เปิดเผยบัญชีและรหัสผ่านของตนกับผู้อื่นที่ใช้คอมพิวเตอร์ร่วมกัน

2. การจัดการความปลอดภัยของข้อมูล

- วัตถุประสงค์

กำหนดโครงสร้างการบริหารจัดการเพื่อความมั่นคงทางเทคโนโลยีสารสนเทศภายในองค์กร

- แนวทางปฏิบัติ

- ผู้บริหารระดับสูงจะดูแลการปฏิบัติตามนโยบายและแนวทางความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

- ผู้จัดการ – หัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะมอบหมายงานให้กับผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจในความปลอดภัยและควบคุมการปฏิบัติงานตามที่กำหนดไว้ในนโยบายและแนวทางการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ

- ผู้จัดการ – หัวหน้าแผนกเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการจัดการ ควบคุม ตรวจสอบ และทบทวนนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยรวม

- เจ้าหน้าที่เทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบต้องตรวจสอบและรับรองความปลอดภัยของระบบ ในกรณีที่เกิดเหตุการณ์ด้านความปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด พวกเขาจะต้องแก้ไขปัญหาและรายงานไปยังผู้บังคับบัญชา

- ผู้ใช้ รวมถึงสำนักงานภายในและภายนอกต้องปฏิบัติตามนโยบายและแนวทางการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท และต้องไม่กระทำการใด ๆ ที่ฝ่าฝืนกฎหมายว่าด้วยอาชญากรรมทางอินเทอร์เน็ต ซึ่งรวมถึงแต่ไม่จำกัดพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคลและพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์

3. ความมั่นคงด้านทรัพยากรมนุษย์

- วัตถุประสงค์

เพื่อให้แน่ใจว่า ผู้ใช้ทุกคนเข้าใจบทบาทและหน้าที่ความรับผิดชอบของตนเมื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

- แนวทางปฏิบัติ

1. กำหนดกฎเกณฑ์ และความรับผิดชอบต่างๆ ให้เป็นลายลักษณ์อักษรสำหรับพนักงานหรือผู้รับเหมา โดยจะต้องสอดคล้องกับนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

2. ให้พนักงานและหน่วยงานในแผนกต่างๆ ลงนามในสัญญาการห้ามเปิดเผยข้อมูล (เอ็นดีเอ) โดยถือว่าเป็นส่วนหนึ่งของการจ้างงาน(เอ็นดีเอส) ผูกมัดให้พนักงานเก็บข้อมูลเป็นความลับในขณะที่พวกเขาทำงานให้กับบริษัท และอย่างน้อย 1 ปีหลังจากการเลิกจ้าง

3. ขอให้ฝ่ายทรัพยากรบุคคลหรือสำนักงานต่างๆ ที่เกี่ยวข้องรายงานต่อผู้จัดการด้านเทคโนโลยีสารสนเทศทันทีในกรณีที่เกิดเหตุการณ์ต่อไปนี้ เพื่อให้แน่ใจว่าได้จัดการบัญชีผู้ใช้ที่ถูกต้องและทันสมัยที่สุด:

- การจ้างงาน
- การเปลี่ยนแปลงเงื่อนไขการจ้างงาน
- การลาออกหรือการเลิกดำรงตำแหน่งกรรมการหรือการจ้างงาน
- การโอนย้าย

4. พนักงานและผู้รับเหมาต้องรับทราบนโยบายที่เกี่ยวข้องกับการจัดการความปลอดภัยของเทคโนโลยีสารสนเทศ

5. พนักงานใหม่จะต้องได้รับการฝึกอบรมในเรื่องนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งควรเป็นส่วนหนึ่งของการปฐมนิเทศ

6. การเข้าถึงข้อมูลจะต้องถูกยกเลิกทันทีหลังการเปลี่ยนแปลง หรือมีการยุติการจ้างงานหรือเมื่อสิ้นสุดโครงการ

5 การบริหารจัดการทรัพย์สินทางด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของข้อนี้คือเพื่อแจ้งให้ผู้ใช้ทราบถึงบทบาทและหน้าที่ความรับผิดชอบในการใช้คอมพิวเตอร์และอุปกรณ์ต่อพ่วงของบริษัทฯ ตลอดจนความจำเป็นในการปฏิบัติตามกฎเกณฑ์อย่างเคร่งครัด เพื่อให้ทรัพยากรและข้อมูลของบริษัทยังคงมีความปลอดภัย และถูกต้องพร้อมใช้งาน

- ผู้ใช้คอมพิวเตอร์และอุปกรณ์ต่อพ่วงของบริษัทเป็นผู้รับผิดชอบสำหรับเครื่องเหล่านี้
- ห้ามใช้คอมพิวเตอร์และเครือข่ายของบริษัทเพื่อวัตถุประสงค์ทางธุรกิจส่วนตัวต่างๆ หรือให้บริการที่ไม่เหมาะสม
- ห้ามไม่ให้ผู้ใช้บริการทำการติดตั้งซอฟต์แวร์ใหม่หรือเปลี่ยนโปรแกรมที่ติดตั้งในคอมพิวเตอร์ของบริษัท เว้นแต่จะขอคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบหรือได้รับอนุญาตจากฝ่ายบริหาร
- ห้ามดัดแปลงแก้ไขคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบหรือหน่วยงานที่รับผิดชอบผู้ใช้จะต้องรักษาคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้อยู่ในสภาพดี
- ผู้ใช้ต้องไม่เก็บหรือใช้คอมพิวเตอร์ในสภาพแวดล้อมที่ร้อน ชื้น มีฝุ่นเยอะ และหลีกเลี่ยงการทำอุปกรณ์ตก
- งดใช้หรือวางอุปกรณ์ใกล้ของเหลว สนามแม่เหล็ก ไฟฟ้าแรงสูง พื้นผิวสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- เคลื่อนย้ายคอมพิวเตอร์ด้วยความระมัดระวัง อย่าวางของหนักทับหรือโยนคอมพิวเตอร์
- ห้ามเคลื่อนย้ายในขณะที่ฮาร์ดดิสก์ยังใช้งานอยู่หรือเปิดเครื่องอยู่
- วางหน้าจอคอมพิวเตอร์ให้ห่างจากวัตถุของแข็ง เพื่อหลีกเลี่ยงการเกิดรอยขีดข่วนหรือความเสียหาย ค่อยๆเช็ดทำความสะอาดหน้าจอด้วยผ้าในทิศทางเดียวกัน การหมุนผ้าเป็นวงกลมอาจทำให้เกิดรอยขีดข่วนได้
- ผู้ใช้ต้องส่งคืนคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่อยู่ในความครอบครองไปยังหน่วยงานที่รับผิดชอบเมื่อมีการเลิกจ้างงาน หรือโครงการสัญญาสิ้นสุดลง โดยที่อุปกรณ์ต่างๆต้องอยู่ในสภาพดี

- ปฏิบัติตามกฎของบริษัทฯ ที่เกี่ยวกับการใช้ทรัพย์สินของบริษัทนอกสถานที่เมื่อมีความจำเป็นต้องนำคอมพิวเตอร์ออกจากสถานที่

- ผู้ใช้จะต้องรับผิดชอบต่อการสูญหายพวกเขาไม่ควรทิ้งคอมพิวเตอร์ไว้ในที่สาธารณะหรือในสถานที่ที่มีความเสี่ยงสูงต่อการสูญหาย

6 ใบอนุญาตใช้ซอฟต์แวร์ถูกลิขสิทธิ์

วัตถุประสงค์ของข้อนี้คือการเพิ่มความตระหนักในบทบาทและหน้าที่ความรับผิดชอบของผู้ใช้ซอฟต์แวร์คอมพิวเตอร์ และเพื่อให้แน่ใจว่าผู้ใช้งานมีความเข้าใจการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์โดยปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัดและรักษาความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

บทบาทและหน้าที่ความรับผิดชอบของผู้ดูแลระบบ

- รับผิดชอบในการควบคุมการใช้ซอฟต์แวร์และการจัดสรรซอฟต์แวร์ตามสิทธิของผู้ใช้

- รับผิดชอบการติดตั้งและการอัพเกรดซอฟต์แวร์สำหรับผู้ใช้ตามตารางเวลาที่กำหนดไว้

- ลบและยกเลิกการเข้าถึงซอฟต์แวร์ทันทีหลังจากได้รับการแจ้งเตือนจากบริษัทและ/หรือแผนก

บทบาทและหน้าที่ความรับผิดชอบของผู้ใช้

- ใช้คอมพิวเตอร์ราวกับว่าเป็นทรัพย์สินของตนเองโดยไม่กระทำการที่ผิดกฎหมายซึ่งอาจเป็นอันตรายต่อบริษัท

- โปรแกรมที่ติดตั้งบนคอมพิวเตอร์ของบริษัทคือโปรแกรมที่ซื้อมาพร้อมกับใบอนุญาตให้ใช้งานที่ถูกต้องดังนั้นจึงห้ามมิให้ผู้ใช้งานทำการคัดลอกโปรแกรมและติดตั้งโปรแกรมบนคอมพิวเตอร์เครื่องอื่นหรือปรับเปลี่ยนแก้ไขโปรแกรมเหล่านั้น

- ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมละเมิดลิขสิทธิ์ และชุดคำสั่งใดๆโดยไม่ได้รับอนุญาต โดยเฉพาะการตกเป็นเครื่องมือในความกระทำผิดทางกฎหมาย

- การติดตั้งโปรแกรมที่ผิดกฎหมายบนคอมพิวเตอร์เป็นสิ่งต้องห้ามอย่างเคร่งครัดหากผู้ใช้รายใดมีการใช้โปรแกรมอื่นนอกเหนือจากโปรแกรมที่ติดตั้งไว้ไม่ว่าจะเป็นโปรแกรมที่ได้รับอนุญาตหรือฟรีแวร์ก็ตาม ผู้ใช้จะต้องรับผิดชอบต่อความเสียหายหรือการละเมิดที่อาจเกิดขึ้นเพียงผู้เดียว

- ผู้ใช้จะต้องส่งคำขอแยกต่างหากสำหรับการติดตั้งการยกเลิกการถ่ายโอนการส่งคืนคอมพิวเตอร์และโปรแกรมให้กับผู้มีอำนาจและผู้ดูแลระบบซึ่งมีหน้าที่รับผิดชอบในการดำเนินการตามคำขอที่ได้รับการอนุมัติเป็นกรณี ๆ ไป

7 การควบคุมการเข้าถึงคอมพิวเตอร์และเซิร์ฟเวอร์

วัตถุประสงค์ของข้อ คือเพื่อใช้เป็นแนวทางเกี่ยวกับสินทรัพย์ทางข้อมูลที่ไม่ได้ใช้- เอกสาร สื่อบันทึก คอมพิวเตอร์และข้อมูล – จะต้องถูกเก็บให้ปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตโดยผู้ใช้จะต้องออกจากระบบเทคโนโลยีสารสนเทศเมื่อไม่ได้ใช้งาน ภายใต้แนวทางต่างๆ ดังต่อไปนี้

1. ออกจากระบบทันทีเมื่อเสร็จสิ้นการใช้งาน

2. มีการตรวจสอบความถูกต้องอย่างที่ควรก่อนใช้งาน เพื่อป้องกันคอมพิวเตอร์

3. บันทึกและจัดเก็บข้อมูลที่สำคัญของแผนกต่างๆที่เกี่ยวข้อง โดยการจัดเก็บข้อมูลสามารถเก็บได้ในรูปแบบต่อไปนี้:

- ในฐานข้อมูลของระบบแอปพลิเคชันที่ครอบคลุมโดยศูนย์ข้อมูลของบริษัท ซึ่งจะป้องกันการส่งข้อมูลออกไป

- ในไฟล์ที่ใช้ร่วมกัน (ไดรฟ์กลาง) ในโฟลเดอร์ที่สามารถเข้าถึงได้ตามสิทธิ์ของผู้ใช้

4. ปิดเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งานนานกว่าหนึ่งชั่วโมงหรือเมื่อทำงานประจำวันแล้วเสร็จยกเว้นเซิร์ฟเวอร์คอมพิวเตอร์ที่ต้องทำงานตลอดเวลา

5. ตั้งค่าโปรแกรมรักษาหน้าจอให้ปิดหน้าจออัตโนมัติหลังจากไม่มีการใช้งานเกินกว่า 10 นาที

6. ขออนุมัติจากหัวหน้าแผนกหรือผู้มีอำนาจสูงกว่าเมื่อใดก็ตามที่ต้องการย้ายสินทรัพย์ข้อมูล – เอกสาร สื่อบันทึก และอุปกรณ์คอมพิวเตอร์ – ออกจากบริษัท โดยกระบวนการดังกล่าวต้องเป็นไปตามกฎการโอนเข้า/โอนออกสินทรัพย์ของบริษัท

7. ให้ระมัดระวังและดูแลทรัพย์สินของบริษัทฯ โดยถือเสมือนว่าเป็นทรัพย์สินของตนเองในกรณีที่เกิดการสูญหายเนื่องจากความประมาทเลินเล่อ พวกเขาจะต้องรับผิดชอบหรือชดใช้ค่าเสียหาย

7 จดหมายอิเล็กทรอนิกส์ (อีเมล)

วัตถุประสงค์ของข้อนี้คือเพื่อให้มั่นใจว่าการส่งข้อความจดหมายอิเล็กทรอนิกส์ (อีเมล) ที่เหมาะสมสะดวกรวดเร็วทันเวลานั้น มีประสิทธิภาพและปลอดภัยเพื่อสนับสนุนการดำเนินงานตามแนวทางของกฎหมายกฎระเบียบกฎและมาตรการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท และเพื่อให้ผู้ใช้เข้าใจและคำนึงถึงปัญหาที่เกิดจากการใช้จดหมายอิเล็กทรอนิกส์บนอินเทอร์เน็ตผู้ใช้จึงจะต้องเข้าใจกฎที่ถูกกำหนดขึ้นไว้โดยผู้ดูแลระบบและไม่ทำการละเมิดกฎหรือพยายามดำเนินการใด ๆ ที่จะก่อให้เกิดปัญหาหรือผิดกฎได้ โดยจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

1. ผู้ใช้อีเมลต้องไม่ฝ่าฝืนพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและกฎเกณฑ์ด้านเทคโนโลยีสารสนเทศของบริษัท

2. หน่วยธุรกิจหรือพนักงานต่างๆที่ส่งข้อความทางอีเมลของบริษัท จำต้องใช้อีเมลเพื่อผลประโยชน์ของบริษัท

3. พนักงานมีสิทธิ์ในการใช้อีเมล ผู้ดูแลระบบจะทำการลงทะเบียนให้เสร็จสมบูรณ์ตามรายชื่อพนักงานจากกองทรัพยากรบุคคล

4. ห้ามใช้ที่อยู่อีเมลของผู้อื่นเพื่อส่งหรือรับอีเมลโดยไม่ได้รับความยินยอมจากเจ้าของที่อยู่ในกรณีนี้เจ้าของที่อยู่จะต้องเป็นผู้รับผิดชอบต่อการใช้งาน

5. ผู้ใช้ต้องงดเว้นจากการปลอมแปลงและหลอกลวงในการใช้อีเมล

6. ในการส่งอีเมลตามที่ได้รับมอบหมายจากบริษัท ผู้ส่งจะต้องใช้ที่อยู่อีเมลของบริษัทเท่านั้น ยกเว้นกรณีเมื่อระบบอีเมลของบริษัททำงานผิดปกติ และผู้บังคับบัญชาอนุมัติการใช้ที่อยู่อีเมลอื่น ๆได้

7. การใช้อีเมลต้องใช้ภาษาที่สุภาพ ต้องไม่ขัดต่อศีลธรรมที่ดีห้ามยั่วยุ เสียดสี หรือฝ่าฝืนกฎหมาย ผู้ใช้ต้องไม่ส่งความเห็นส่วนตัวโดยอ้างว่าเป็นความเห็นของบริษัท ซึ่งอาจทำให้เกิดความเสียหายต่อบริษัทได้

8. ห้ามใช้อีเมลของบริษัทในการเผยแพร่ข้อมูล ข่าวสาร รูปภาพ และอื่นใด ที่เป็นการขัดต่อคุณธรรมจริยธรรมอันดี ความมั่นคงของชาติ และหมิ่นพระบรมเดชานุภาพ ซึ่งเป็นอันตรายต่อการดำเนินงานของบริษัทหรือรบกวนผู้อื่น และรวมถึงผู้รับบริการของบริษัท

9. ห้ามมิให้ผู้ใช้ใช้ที่อยู่อีเมลสำหรับกิจกรรมส่วนตัวเช่นการทำธุรกิจส่วนตัวและการลงทะเบียนโซเชียลมีเดียหากมีการตรวจพบการกระทำดังกล่าวเจ้าของอีเมลหรือผู้ใช้จะต้องเป็นผู้รับผิดชอบ

10. ห้ามมิให้ดำเนินการใด ๆ ที่จะก่อให้เกิดปัญหากับทรัพยากรของระบบเช่นการสร้างจดหมายลูกโซ่การส่งจดหมายขยะ การส่งระเบิดจดหมายหรือส่งอีเมลเพื่อแพร่กระจายไวรัสคอมพิวเตอร์

11. ห้ามส่งข้อมูลที่เป็นความลับของบริษัทให้แก่บุคคลอื่นหรือหน่วยงานอื่นที่ไม่เกี่ยวข้องกับภารกิจของบริษัท

12. หากมีการส่งข้อมูลที่เป็นความลับจะต้องผ่านการเข้ารหัสก่อน และความสำคัญของข้อมูลดังกล่าวจะไม่ถูกระบุในส่วนหัวของอีเมล

13. ต้องทำการออกจากระบบเสมอหลังจากเสร็จสิ้นการใช้อีเมล

14. บริษัทขอสงวนสิทธิ์ในการยกเลิกหรือระงับการให้บริการอีเมลแก่พนักงานเมื่อได้รับการร้องเรียนและคำขอหรือเมื่อพบการกระทำที่ผิดกฎหมายการสืบสวนจะเริ่มต้นขึ้น

15. หากพบเห็นกิจกรรมที่ไม่เหมาะสมหรือมีการล่วงละเมิด ผู้ใช้จะต้องยื่นรายงานต่อช่องทางการแจ้งเบาะแสของบริษัท

16. ผู้ใช้จำเป็นต้องรับผิดชอบต่อการกระทำใดๆ ที่เกี่ยวข้องกับการแจกจ่าย ทั้งในรูปแบบของอีเมลและโฮมเพจของผู้ใช้โดยผู้ดูแลระบบและบริษัทจะไม่มีส่วนเกี่ยวข้องใดๆ

7 การเข้าถึงข้อมูลและสารสนเทศ

วัตถุประสงค์ของข้อนี้คือ เพื่อร่างมาตรการการใช้อินเทอร์เน็ตผ่านเครือข่ายของบริษัทเพื่อประสิทธิภาพและความปลอดภัย และสร้างการรับรู้ของผู้ใช้บริการในการเข้าถึงเว็บไซต์โดยผ่านเครือข่ายของบริษัท

1. ฝ่ายเทคโนโลยีสารสนเทศควรวางเส้นทางการเชื่อมต่ออินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยเช่นไฟร์วอลล์หรือร็อกซี่เซิร์ฟเวอร์

2. จำเป็นต้องติดตั้งโปรแกรมป้องกันไวรัสและต้องระบุช่องโหว่ก่อนที่จะทำการเชื่อมต่อคอมพิวเตอร์ของบริษัทกับเครือข่าย

3. หลังจากใช้อินเทอร์เน็ตผู้ใช้จะต้องทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าถึงโดยบุคคลอื่น

4. ผู้ใช้จะต้องเข้าถึงข้อมูลที่เห็นว่าเหมาะสมกับบทบาทและหน้าที่ความรับผิดชอบของตน เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยของบริษัท

5. ห้ามมิให้ผู้ใช้เปิดเผยข้อมูลที่เป็นความลับของบริษัท เว้นแต่จะเป็นไปตามหลักเกณฑ์การเปิดเผยข้อมูลอย่างเป็นทางการของบริษัท

6. ผู้ใช้จะต้องระมัดระวังในการดาวน์โหลดโปรแกรมผ่านอินเทอร์เน็ต รวมถึงการดาวน์โหลดเพื่ออัพเดตโปรแกรม โดยต้องตระหนักว่าการดาวน์โหลดดังกล่าวจะต้องไม่เป็นการละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น

7. ผู้ใช้จะต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลบนอินเทอร์เน็ตก่อนที่จะใช้งาน

8. ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทเพื่อผลประโยชน์ทางธุรกิจส่วนตัว หรือเพื่อเข้าถึงเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดีหรือผู้ที่มีข้อมูลที่เป็นอันตรายต่อความมั่นคงของชาติ ศาสนา สถาบันพระมหากษัตริย์และสังคม ตลอดจนเว็บไซต์ลามกอนาจาร

9. ผู้ใช้อินเทอร์เน็ตจะไม่ละเมิดผู้อื่นหรือก่อให้เกิดความเสียหายต่อบริษัทผู้ใช้จะไม่กระทำการอันเป็นการฝ่าฝืนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือกฎหมายที่เกี่ยวข้อง ในการใช้อินเทอร์เน็ตเพื่อสนับสนุนการมอบหมายงาน ผู้ใช้ต้องปฏิบัติตามขั้นตอนที่บริษัทกำหนดอย่างเคร่งครัด

8 การเข้ารหัสลับและการควบคุมที่เกี่ยวข้อง

A. การจัดการบริหารข้อมูล

1. ข้อมูลที่เป็นความลับจะต้องถูกจัดประเภทตามภารกิจและความสำคัญ โดยการจัดการของแต่ละประเภทจะต้องถูกกำหนดด้วยวิธีการจัดการข้อมูลลับหรือข้อมูลที่สำคัญก่อนที่จะมีการยกเลิกหรือนำกลับมาใช้ใหม่

2. ข้อมูลสำคัญที่ส่งผ่านเครือข่ายสาธารณะจะต้องได้รับการเข้ารหัสด้วยมาตรฐานการเข้ารหัสระหว่างประเทศ เช่น ระบบการเข้ารหัสข้อมูลเพื่อเพิ่มความปลอดภัย (เอส เอส แอล) และระบบรับส่งข้อมูลภายในองค์กรจากระยะไกลได้โดยที่ความปลอดภัยของข้อมูลยังคงอยู่(วีพีเอ็น)

3. ต้องมีมาตรการควบคุมความถูกต้องและความสอดคล้องของข้อมูลเข้าและส่งออก ในกรณีที่ข้อมูลถูกเก็บไว้มากกว่าหนึ่งแห่ง (ฐานข้อมูลแบบกระจาย) หรือเกี่ยวข้องกับชุดข้อมูลอื่น

4. ในกรณีที่คอมพิวเตอร์ถูกย้ายออกจากสถานที่ของบริษัทเพื่อการซ่อมแซมหรือเพื่อวัตถุประสงค์อื่นควรมีการวางมาตรการรักษาความปลอดภัยของข้อมูลเช่น อาจจำเป็นต้องลบข้อมูลบางอย่างออกไป

บี. การควบคุมสิทธิ์ของผู้ใช้

1. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์การประมวลผลโดยคำนึงถึงการใช้งานและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ กำหนดกฎระเบียบสำหรับการเข้าถึงและสิทธิพิเศษสำหรับพนักงานทุกระดับที่ต้องรับทราบและปฏิบัติตามอย่างเคร่งครัด ซึ่งพนักงานควรตระหนักถึงความสำคัญของระบบรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2. กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของพนักงาน ตัวอย่างเช่น การเข้าถึงระบบแอปพลิเคชันและการเข้าถึงอินเทอร์เน็ตตามบทบาทและความรับผิดชอบ ให้สิทธิ์การเข้าถึงแก่พนักงานเพื่อทำงานที่จำเป็นเท่านั้น โดยได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้รับผิดชอบ โดยมีการตวจสอบสิทธิ์การเข้าถึงเป็นระยะๆ

3. หากผู้ใช้ต้องการสิทธิพิเศษในการเข้าถึง ผู้ใช้จะต้องถูกควบคุมอย่างเคร่งครัด โดยพิจารณาปัจจัยต่อไปนี้เพื่อตรวจสอบว่ามาตรการควบคุมที่มีนั้นมีความเข้มงวดเพียงพอหรือไม่

- ได้รับการอนุมัติจากผู้มีอำนาจ
- มีการเข้าถึงที่เข้มงวด เช่น เมื่อจำเป็นเท่านั้น
- การตั้งค่าจำกัดเวลาและจะยกเลิกการเข้าถึงทันทีเมื่อเวลาหมด
- ทำการเปลี่ยนรหัสผ่านเป็นระยะๆ ตัวอย่างเช่นหลังจากที่งานแล้วเสร็จหรือเปลี่ยนทุก6เดือน หากจำเป็นต้องมีการเข้าถึงในระยะเวลานาน

4. กำหนดมาตรการเพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงคอมพิวเตอร์ในขณะที่ผู้ใช้ที่ได้รับอนุญาตไม่อยู่ ตัวอย่างเช่นผู้ใช้ที่ได้รับอนุญาตจะต้องออกจากระบบก่อนออกจากคอมพิวเตอร์

5. ในกรณีที่จำเป็นสำหรับผู้ใช้ที่มีข้อมูลที่สำคัญที่เป็นความลับ จะต้องอนุญาตให้ผู้ใช้อื่นๆ เข้าถึงเพื่อแก้ไขข้อมูลของตนได้ เช่น ผ่านไฟล์ที่แชร์ การเข้าถึงดังกล่าวจะถูกจำกัดเฉพาะบุคคลหรือกลุ่มบุคคล และจะต้องถูกยกเลิกเมื่อการเข้าถึงดังกล่าวไม่จำเป็นอีกต่อไป เจ้าของข้อมูลต้องแสดงหลักฐานการอนุญาต กำหนดระยะเวลา และยกเลิกการเข้าถึงทันทีหลังจากเวลาหมด

6. ในกรณีที่จำเป็นต้องให้สิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศหรือเครือข่ายในกรณีฉุกเฉินหรือชั่วคราวจะต้องปฏิบัติตามมาตรการและต้องได้รับอนุญาตจากผู้มีอำนาจตลอดเวลา ทำการบันทึกเหตุผลและความจำเป็นของการอนุญาตดังกล่าว มีกำหนดระยะเวลาการใช้งานและยกเลิกการใช้งานทันทีหลังหมดเวลา

ซี. บัญชีผู้ใช้และการควบคุมรหัสผ่าน

1. กำหนดมาตรการการระบุตัวตนและการอนุมัติตัวตนที่รัดกุม เช่น ตั้งค่ารหัสผ่านที่ยากแก่การคาดเดา ผู้ใช้แต่ละรายต้องมีบัญชีผู้ใช้ของตนเอง ในการพิจารณาว่ารหัสผ่านนั้นคาดเดาได้ยากและการควบคุมรหัสผ่านนั้นยากหรือไม่ บริษัทจะใช้ปัจจัยต่อไปนี้ในการพิจารณาโดยรวม:

- รหัสผ่านควรมีความยาวพอสมควร มาตรฐานสากลส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 อักขระ (ตัวอักษรและตัวเลข)
- ประกอบด้วยอักขระพิเศษ เช่น <,>, $, @ และ #
- ผู้ใช้ทั่วไปควรทำการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ผู้มีสิทธิ์พิเศษ เช่นผู้ดูแลระบบและผู้ใช้เริ่มต้นควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 2 เดือน
- รหัสผ่านใหม่ไม่ควรซ้ำรหัส 3 อันล่าสุด
- รหัสผ่านไม่ควรตั้งตามแบบธรรมดา หรือที่คาดเดาได้ เช่น “abcdef”, “aaaaaa”, “123456”, “password” หรือ “P@ssw0rd”
- รหัสผ่านไม่ควรมีข้อมูลของผู้ใช้ เช่น ชื่อ นามสกุล วันเดือนปีเกิด และที่อยู่
- รหัสผ่านต้องไม่ใช่คำศัพท์ที่ปรากฏในพจนานุกรม
- กำหนดจำนวนครั้งที่ผู้ใช้ได้รับอนุญาตให้ป้อนรหัสผ่านผิดโดยทั่วไปจะจำกัดอยู่ที่ 5 ครั้ง หากใส่รหัสผ่านผิดเกินกว่ากำหนดระบบหรือโปรแกรมจะถูกปิดกั้น
- ใช้วิธีการที่ฉลาดและปลอดภัยในการส่งรหัสผ่านให้กับผู้ใช้ เช่น ผ่านซองจดหมายที่ปิดผนึก
- หลังจากได้รับรหัสผ่านเริ่มต้นหรือรหัสผ่านใหม่ผู้ใช้ควรเปลี่ยนรหัสผ่านทันที
- ผู้ใช้ควรเก็บรหัสผ่านเป็นความลับ อย่าเขียนรหัสผ่านลงบนกระดาษแล้วติดลงบนหน้าจอ หากผู้อื่นทราบรหัสผ่านผู้ใช้ควรเปลี่ยนรหัสผ่านทันที
- กรณีแชร์สิทธิ์การใช้งานร่วมกัน เช่น ระบบเอสเอพีผู้ดูแลระบบจะส่งอีเมลแจ้งไปยังผู้รับผิดชอบเพื่อเปลี่ยนรหัสผ่านเมื่อมีการเปลี่ยนแปลงผู้ใช้ในเครือ

2. ไฟล์ที่จัดเก็บรหัสผ่านจำเป็นต้องมีการเข้ารหัส เพื่อความปลอดภัยจากการรั่วไหลหรือการดัดแปลง

3. ทำการตรวจสอบรายชื่อผู้ใช้ระบบที่สำคัญเป็นประจำ ตรวจสอบรายชื่อผู้ใช้สิทธิ์ที่ถูกเลิกจ้าง รวมถึงผู้ใช้ที่ลาออกและผู้ใช้เริ่มต้น ระงับผู้ใช้ทันทีเมื่อตรวจพบโดยปิดใช้งานการเข้าถึง ลบออก เปลี่ยนรหัสผ่าน ฯลฯ

9 ความปลอดภัยทางกายภาพ

วัตถุประสงค์ของการควบคุมการเข้าถึงห้องศูนย์ข้อมูลเพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตในการเข้าถึง มีการรับรู้ เปลี่ยนแปลงหรือทำลายข้อมูลและเครือข่ายคอมพิวเตอร์การป้องกันความเสียหายมีจุดมุ่งหมายเพื่อปกป้องข้อมูลและเครือข่ายจากภัยพิบัติหรือจากปัจจัยอื่นๆ โดยในส่วนนี้ครอบคลุมถึงมาตรการควบคุมการเข้าถึงสำหรับห้องศูนย์ข้อมูลและระบบป้องกันที่บริษัทควรจัดให้มีในห้องศูนย์ข้อมูล

เอ. ศูนย์ข้อมูล/ การควบคุมห้องเซิร์ฟเวอร์

1. อุปกรณ์คอมพิวเตอร์ที่สำคัญเช่นเซิร์ฟเวอร์และอุปกรณ์เครือข่ายจะต้องจัดเก็บอยู่ในห้องศูนย์ข้อมูลหรือพื้นที่หวงห้าม การเข้าถึงห้องศูนย์ข้อมูลควรจำกัดเฉพาะผู้รับผิดชอบ เช่น ผู้ดูแลระบบเท่านั้น

2. ต้องมีมาตรการหากบุคคลที่ไม่มีหน้าที่ประจำจำเป็นต้องเข้าถึงห้องศูนย์ข้อมูลเป็นครั้งคราว ตัวอย่างเช่นกำหนดให้ผู้ดูแลระบบและ/หรือผู้ดำเนินการที่เกี่ยวข้องกำกับดูแลงานดังกล่าวอย่างละเอียด

3. ควรมีการบันทึกการเข้าใช้ห้องศูนย์ข้อมูล โดยมีรายละเอียดของบุคคลที่เกี่ยวข้องและเวลาที่เข้าและออก ควรมีการตรวจสอบบันทึกเป็นประจำ

4. ห้องศูนย์ข้อมูลควรแบ่งออกเป็นส่วนต่างๆ แยกกัน สำหรับพื้นที่สำหรับเครือข่าย พื้นที่สำหรับเซิร์ฟเวอร์ พื้นที่สำหรับยูพีเอสและพื้นที่สำหรับยูพีเอสแบบแบตเตอร์ และพื้นที่อื่นๆ เพื่อความสะดวกในการใช้งานและควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญได้อย่างมีประสิทธิภาพมากขึ้น

บี. ระบบป้องกันความเสียหาย

1. ระบบป้องกันอัคคีภัย

- ต้องติดตั้งระบบสัญญาณเตือนอัคคีภัย โดยมีการตรวจจับควันและตรวจจับความร้อนเพื่อป้องกันหรือดับไฟได้ทันที

- ห้องศูนย์ข้อมูลหลักจะต้องติดตั้งเครื่องดับเพลิงอัตโนมัติ ที่ศูนย์รอง อย่างน้อยต้องมีเครื่องดับเพลิงเพื่อจัดการกับเหตุการณ์ไฟไหม้ได้ก่อน

2. ระบบป้องกันไฟดับ

- ติดตั้งระบบเพื่อปกป้องคอมพิวเตอร์จากความเสียหายที่อาจเกิดขึ้นจากไฟดับ

- ติดตั้งระบบสำรองไฟสำหรับคอมพิวเตอร์หลักและเครือข่าย เพื่อให้แน่ใจว่าการทำงานไม่ขาดตอน

3. ระบบควบคุมอุณหภูมิและความชื้น

- รักษาระดับอุณหภูมิและความชื้นที่เหมาะสมโดยการตั้งค่าระดับการควบคุมอุณหภูมิและความชื้นของเครื่องปรับอากาศให้สอดคล้องกับข้อกำหนดของระบบคอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์อาจไม่สามารถทำงานได้อย่างราบรื่นภายใต้อุณหภูมิและความชื้นที่ไม่เหมาะสม

4. ระบบเตือนน้ำรั่ว

- กรณีที่พื้นห้องศูนย์ข้อมูลถูกยกสูงเพื่อติดตั้งเครื่องปรับอากาศ สายไฟ และสายไฟใต้พื้น ควรติดตั้งระบบเตือนน้ำรั่วเพื่อป้องกันหรือจัดการการรั่วไหลในทันที หากศูนย์ข้อมูล/ห้องเซิร์ฟเวอร์อยู่ในสถานที่ที่เสี่ยงต่อการรั่วไหลของน้ำ ขอแนะนำให้ตรวจสอบการรั่วไหลที่อาจเกิดขึ้นเป็นประจำ

10 ความปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของข้อนี้คือ เพื่อให้แน่ใจว่าระบบเทคโนโลยีสารสนเทศของบริษัททำงานอย่างเหมาะสมและปลอดภัย ซึ่งจะป้องกันการสูญหายของข้อมูลและปกป้องระบบจากโปรแกรมที่ไม่พึงประสงค์ซึ่งเป็นอันตรายได้ (มัลแวร์)

1. จัดทำคู่มือหรือขั้นตอนเกี่ยวกับระบบเทคโนโลยีสารสนเทศที่สำคัญของบริษัท เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน

2. ควบคุมการแก้ไขปรับเปลี่ยนข้อมูล เช่น ข้อกำหนดในการขออนุมัติจากผู้บังคับบัญชาก่อนการดำเนินการ

3. สำรองข้อมูลก่อนการปรับเปลี่ยนแก้ไข

4. ติดตั้งระบบตรวจสอบเพื่อตรวจสอบความเพียงพอของทรัพยากรของระบบเทคโนโลยีสารสนเทศ เช่น ซีพียู หน่วยความจำ และฮาร์ดดิสก์ และใช้ผลลัพธ์ในการวางแผนในอนาคตเพื่อพิจารณาว่าจะเพิ่มหรือลดทรัพยากร

5. แยกการพัฒนาระบบที่สำคัญออกจากระบบปฏิบัติการรายวัน เพื่อป้องกันการปรับเปลี่ยนแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

6. สำรวจและจำแนกระดับข้อมูล และกำหนดข้อมูลที่ต้องสำรองและความถี่ของการสำรองข้อมูล

7. ข้อมูลสำคัญควรสำรองไว้บ่อยๆ บริษัทควรมีระบบสำรองข้อมูลไว้นอกสถานที่

8. ตรวจสอบความพร้อมของระบบสำรองข้อมูลไอทีอย่างน้อยปีละครั้ง

9. กำหนดมาตรการป้องกันโปรแกรมที่ไม่พึงประสงค์และเป็นอันตราย (มัลแวร์) นั้นได้รวมถึง

- ติดตั้งโปรแกรมป้องกันไวรัสและจัดการกับช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์ก่อนที่จะเชื่อมต่อคอมพิวเตอร์ส่วนบุคคลหรือโน้ตบุ๊กกับเครือข่ายของบริษัท
- ปรับปรุงระบบปฏิบัติการและโปรแกรมอื่นๆเป็นระยะๆตามโปรแกรมแก้ไขที่ออกให้และ/หรือ การแก้ด่วนเพื่อแก้ไขจุดบกพร่องในโปรแกรม โดยผู้ใช้สามารถดาวน์โหลดอัพเดตจากเว็บไซต์ของบริษัทซอฟต์แวร์
- สแกนไวรัสโดยใช้โปรแกรมป้องกันไวรัสก่อนที่จะส่งหรือรับอีเมล
- ผู้ใช้จะต้องติดตั้งโปรแกรมที่บริษัทเตรียมไว้ ถ้าผู้ใช้ต้องการติดตั้งซอฟต์แวร์เพิ่มเติมต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศเพื่อตรวจสอบความปลอดภัย

11 ความปลอดภัยในการสื่อสาร

วัตถุประสงค์ของข้อนี้คือการปกป้องข้อมูลจากบุคคล ไวรัส และรหัสที่เป็นอันตราย ที่อาจเข้าถึงหรือสร้างความเสียหายให้กับข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศ

1. การจัดการความปลอดภัยเครือข่าย

2. ควบคุมการเข้าถึงเพื่อความปลอดภัยของเครือข่าย

3. จัดเตรียมเครือข่ายแยกสำหรับผู้ใช้ภายในและผู้ใช้ภายนอก

4. ความสมบูรณ์ของการถ่ายโอนข้อมูลผ่านการเข้ารหัสและข้อตกลง

12 การจัดจ้างบุคคลภายนอก

วัตถุประสงค์ของข้อนี้คือ เพื่อปกป้องสินทรัพย์ที่สามารถเข้าถึงได้ของบริษัท จากความเสี่ยงที่เกี่ยวข้องกับการจัดจ้างบุคคลภายนอกในการทำงานด้านเทคโนโลยีสารสนเทศ ในขณะที่ยังรักษาระดับความปลอดภัยและคุณภาพการบริการตามที่ได้ตกลงกันไว้ในข้อตกลงการให้บริการ

1. ร่างกฎเพื่อการรักษาความปลอดภัยของข้อมูลของบริษัท เมื่อจำเป็นต้องให้บุคคลภายนอกเข้าถึงข้อมูลหรือทรัพย์สินของบริษัท โดยกฎดังกล่าวจะต้องสอดคล้องกับข้อกำหนดในข้อตกลงที่เป็นความลับ

2. สื่อสารและบังคับใช้กฎความปลอดภัยของข้อมูลเมื่อจำเป็นต้องให้บุคคลภายนอกเข้าถึงข้อมูลหรือทรัพย์สินของบริษัทก่อนที่จะอนุมัติการเข้าถึง

3. ระบุกำหนดการตรวจสอบบริการ ทบทวน และประเมินผลอย่างสม่ำเสมอในข้อตกลงการบริการ

4. ในกรณีที่มีการเปลี่ยนแปลงข้อตกลงสำหรับระบบที่สำคัญ จำเป็นต้องมีการประเมินความเสี่ยงด้านความปลอดภัย

13 การจัดการเหตุการณ์ความปลอดภัยของข้อมูล

วัตถุประสงค์ของข้อนี้ เพื่อลดความซับซ้อนและวิธีการที่มีประสิทธิภาพในการจัดการสถานการณ์ความปลอดภัยของข้อมูลและแสดงสถานะความปลอดภัย พร้อมชี้จุดอ่อนของระบบเทคโนโลยีสารสนเทศ

1. กำหนดบทบาทและขั้นตอนในการแก้ไขปัญหาเหตุการณ์ด้านความปลอดภัย

2. สร้างช่องทางการสื่อสารที่ชัดเจนโดยผู้ใช้สามารถส่งรายงานเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศได้

3. หากผู้ใช้พบเหตุการณ์ใดๆที่อาจรบกวนความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ กรุณาแจ้งฝ่ายเทคโนโลยีสารสนเทศ

4. ต้องรายงานสถานะความปลอดภัยของระบบเทคโนโลยีสารสนเทศตามความรุนแรงของเหตุการณ์ เหตุการณ์ที่จะส่งผลกระทบต่อผู้ใช้จำนวนมากจะต้องประกาศอย่างรวดเร็ว

5. บันทึกเหตุการณ์การละเมิดความปลอดภัย อย่างน้อยให้แจ้งประเภทของเหตุการณ์ ความถี่ของเหตุการณ์ และค่าความเสียหาย เพื่อให้บริษัทได้เรียนรู้จากบทเรียนและเตรียมมาตรการป้องกัน

6. เก็บและรวบรวมพยานหลักฐานตามหลักเกณฑ์หรือแนวทางเพื่อใช้อ้างอิงในกระบวนการพิจารณาคดีในชั้นศาล

14 การจัดการความต่อเนื่อง

วัตถุประสงค์ของข้อนี้คือเพื่อป้องกันการหยุดชะงักของธุรกิจที่เกิดจากวิกฤติหรือภัยพิบัติต่างๆ และตรวจสอบให้แน่ใจว่าอุปกรณ์ระบบเทคโนโลยีสารสนเทศพร้อมใช้งาน

1. เรียกร้องให้ฝ่ายเทคโนโลยีสารสนเทศจัดทำแผนบรรเทาความไม่แน่นอนและภัยพิบัติที่ระบบเทคโนโลยีสารสนเทศอาจประสบได้ โดยให้สอดคล้องตามแผนการจัดการวิกฤตของบริษัท

2. ประมวลผลและประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลอย่างน้อยปีละ1 ครั้ง

3. ทบทวนแผนความต่อเนื่องอย่างน้อยปีละ 1 ครั้ง

4. ตรวจสอบความพร้อมใช้งานของระบบสำรองข้อมูลอย่างน้อยปีละครั้ง

15 การพัฒนาและการบำรุงรักษา

วัตถุประสงค์ของข้อนี้คือการควบคุมการพัฒนาหรือการปรับเปลี่ยนแก้ไขระบบเทคโนโลยีสารสนเทศเพื่อผลลัพธ์การดำเนินงานที่ถูกต้องและสมบูรณ์ตามข้อกำหนดของผู้ใช้ซึ่งจะลดความเสี่ยงด้านความสมบูรณ์ ซึ่งในส่วนนี้ครอบคลุมกระบวนการพัฒนาหรือแก้ไขโดยรวมตั้งแต่คำขอเพื่อพัฒนา หรือแก้ไขระบบงานจนกว่างานจะเสร็จสมบูรณ์และดำเนินการได้

1. สร้างกระบวนการหรือขั้นตอนที่เป็นลายลักษณ์อักษรสำหรับการพัฒนาหรือแก้ไขระบบงาน โดยอย่างน้อยควรครอบคลุมถึงการเขียนคำขอ การพัฒนาแก้ไขหรือดัดแปลงการทดสอบและกระบวนการโอนย้ายงาน

2. พัฒนาขั้นตอนหรือแนวทางการเปลี่ยนแปลงฉุกเฉินในระบบงานมีการระบุความจำเป็นของการเปลี่ยนแปลงดังกล่าวโดยตลอดเวลา ซึ่งต้องได้รับอนุญาตจากผู้มีอำนาจ

3. สื่อสารรายละเอียดของขั้นตอนเหล่านั้นอย่างละเอียดกับผู้ใช้และผู้ที่เกี่ยวข้องและมีการตรวจสอบการปฏิบัติตาม

• การควบคุมการพัฒนาหรือการปรับปรุงเปลี่ยนแปลง

เอ. การยื่นคำร้อง

• การยื่นคำร้องสำหรับการพัฒนาและการปรับเปลี่ยนระบบงานจะต้องทำเป็นลายลักษณ์อักษรรวมถึงรูปแบบอิเล็กทรอนิกส์ด้วย เช่น การยื่นคำร้องผ่านอีเมลจะได้รับการอนุมัติจากผู้มีอำนาจเช่นหัวหน้างานของแผนกที่ยื่นคำร้องหรือผู้ดูแลระบบ

• ต้องเตรียมการประเมินผลกระทบต่อการดำเนินงานความปลอดภัยและการทำงานของระบบงานที่เกี่ยวข้องจากการเปลี่ยนแปลงดังกล่าวเป็นลายลักษณ์อักษร

• ควรตรวจสอบเพื่อยืนยันความถูกต้องของกฎระเบียบที่เกี่ยวข้องต่างๆที่เป็นทางการเนื่องจากการเปลี่ยนแปลงหลายอย่างอาจรบกวนการปฏิบัติตามกฎอย่างเป็นทางการได้

บี. การพัฒนาระบบงาน

• แยกคอมพิวเตอร์เพื่อวัตถุประสงค์ในการพัฒนาออกจากคอมพิวเตอร์ที่ใช้ปฏิบัติงานและทำการจำกัดการเข้าถึงแต่ละส่วนสำหรับบุคคลที่เกี่ยวข้องเท่านั้น การแยกสามารถทำได้โดยใช้คอมพิวเตอร์สองเครื่องหรือโดยการใช้เนื้อที่ร่วมกันในคอมพิวเตอร์เครื่องเดียว

• ผู้ยื่นคำร้องขอพัฒนาหรือแก้ไขและผู้ใช้ที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการเพื่อให้บรรลุระบบการทำงานที่พึงประสงค์

• ตลอดกระบวนการโดยตั้งแต่ขั้นตอนแรกควรให้ความสำคัญกับความปลอดภัยและความพร้อมของระบบงานเป็นอันดับต้นๆ

ซี. การทดสอบ

• เกี่ยวข้องกับผู้ยื่นคำร้อง และฝ่ายเทคโนโลยีสารสนเทศรวมถึงผู้ใช้ที่เกี่ยวข้องอื่นๆ ในการทดสอบเพื่อให้แน่ใจว่าประสิทธิภาพของระบบงานที่พัฒนาหรือแก้ไขรวมถึงการประมวลผลนั้น ถูกต้องและสมบูรณ์ก่อนที่จะถ่ายโอนงานและเริ่มปฏิบัติการ

ดี. การโอนย้ายงาน

• ทำการตรวจสอบการโอนย้ายงานอย่างสม่ำเสมอ

อี. จัดทำเอกสารและรายละเอียดของขั้นตอนการพัฒนาเพื่อความปลอดภัย

• ทำการเก็บรายละเอียดของโปรแกรมที่ใช้อยู่ในปัจจุบันที่คำนึงถึงการพัฒนาและการปรับเปลี่ยนก่อนหน้านี้

• อัปเดตเอกสารที่เกี่ยวข้องทั้งหมดเป็นประจำหลังจากการพัฒนาหรือแก้ไขแต่ละครั้ง รวมถึงรายละเอียดของโครงสร้างข้อมูล คู่มือระบบการทำงาน การลงทะเบียนผู้ใช้ที่มีสิทธิ์ ขั้นตอนการทำงานของโปรแกรมและข้อกำหนดของโปรแกรม เอกสารต้องเก็บไว้ในที่ปลอดภัยและสะดวก

• เก็บโปรแกรมรุ่นก่อนหน้าที่ได้รับการแก้ไขไว้เพื่อใช้ในกรณีฉุกเฉิน ในกรณีที่รุ่นปัจจุบันมีการผิดพลาดหรือล้มเหลว

เอฟ. การทดสอบหลังการใช้งาน

• กำหนดเวลาการทดสอบในโปรแกรมที่พัฒนาหรือดัดแปลงหลังจากใช้งานในช่วงระยะเวลาหนึ่ง เพื่อให้แน่ใจว่าระบบงานมีประสิทธิภาพ การประมวลผลที่แม่นยำและครบถ้วนและสามารถตอบสนองความต้องการของผู้ใช้ได้

จี. การสื่อสารเรื่องการเปลี่ยนแปลง

• เพื่อแจ้งให้ผู้ใช้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงเพื่อการใช้งานที่ประสบความสำเร็จ

16 การบังคับใช้หลักจรรยาบรรณนี้

กรรมการ ผู้บริหาร พนักงาน และผู้ร่วมงานทุกคน รวมถึงซัพพลายเออร์ หุ้นส่วนกิจการร่วมทุน ที่ปรึกษา และผู้ให้บริการจะต้องปฏิบัติตามหลักจรรยาบรรณนี้ นอกเหนือจากข้อกำหนดเฉพาะ

ใดๆ ตามข้อตกลงที่ลงนามกับ เมก้าในกรณีที่มีความแตกต่างระหว่างหลักจรรยาบรรณนี้กับข้อตกลง/เอกสาร ให้ข้อตกลง/เอกสารมีผลเหนือกว่า

17 การไม่ตอบโต้

เราไม่ยอมให้มีการตอบโต้กับพนักงานหรือผู้มีส่วนได้ส่วนเสียที่ยื่นรายงานเหตุการณ์การไม่ปฏิบัติตามข้อกำหนด รายงานแต่ละฉบับจะได้รับการตรวจสอบอย่างเต็มที่ และใช้มาตรการการแก้ไขที่เหมาะสมเพื่อป้องกันการกระทำผิดเพิ่มเติมและลงโทษสำหรับความคลาดเคลื่อนของข้อมูลในอดีตตามที่การกระทำดังกล่าวได้รับการพิจารณาในการสอบสวนให้มีลักษณะเป็นการประพฤติมิชอบ